

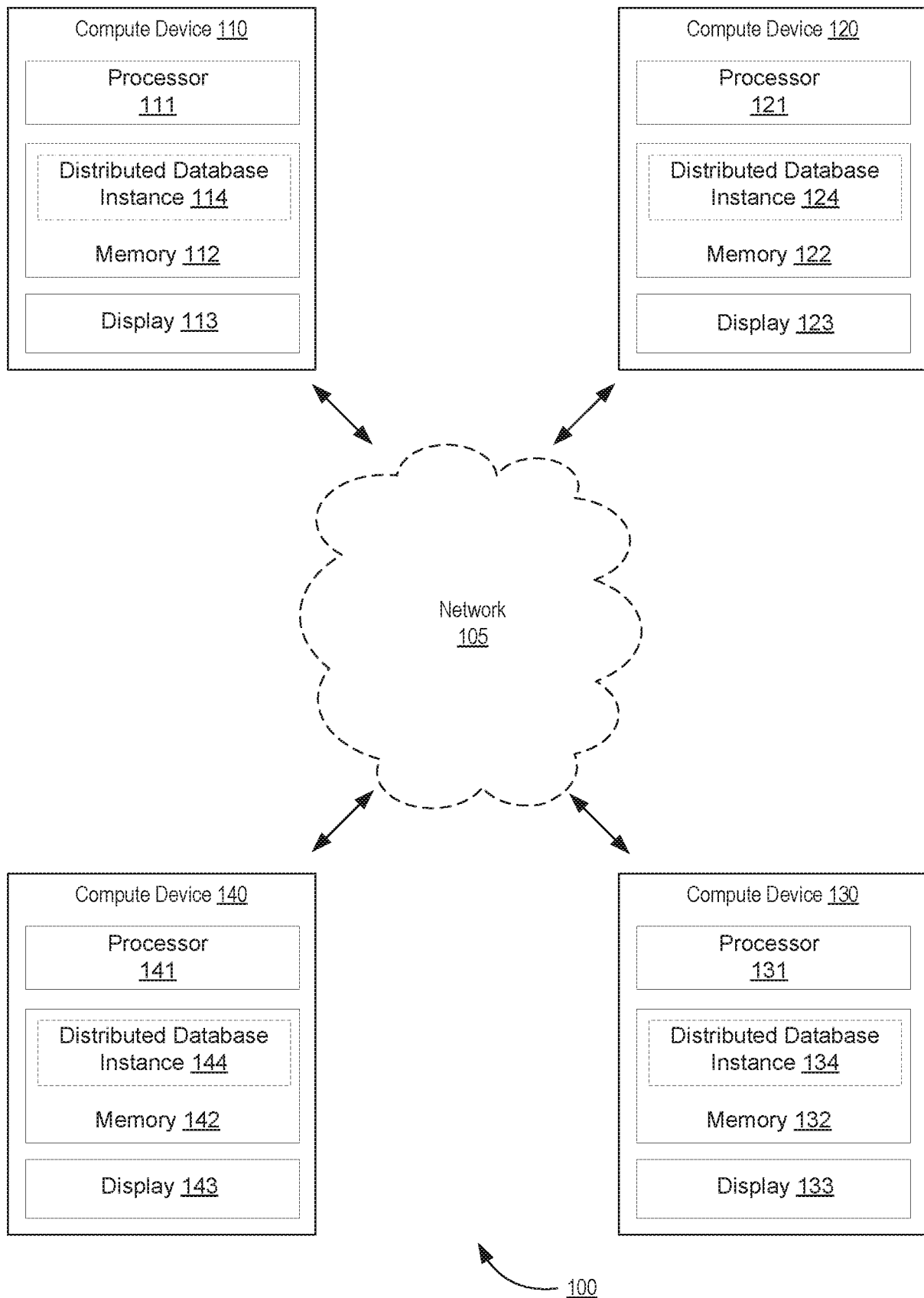


FIG. 1

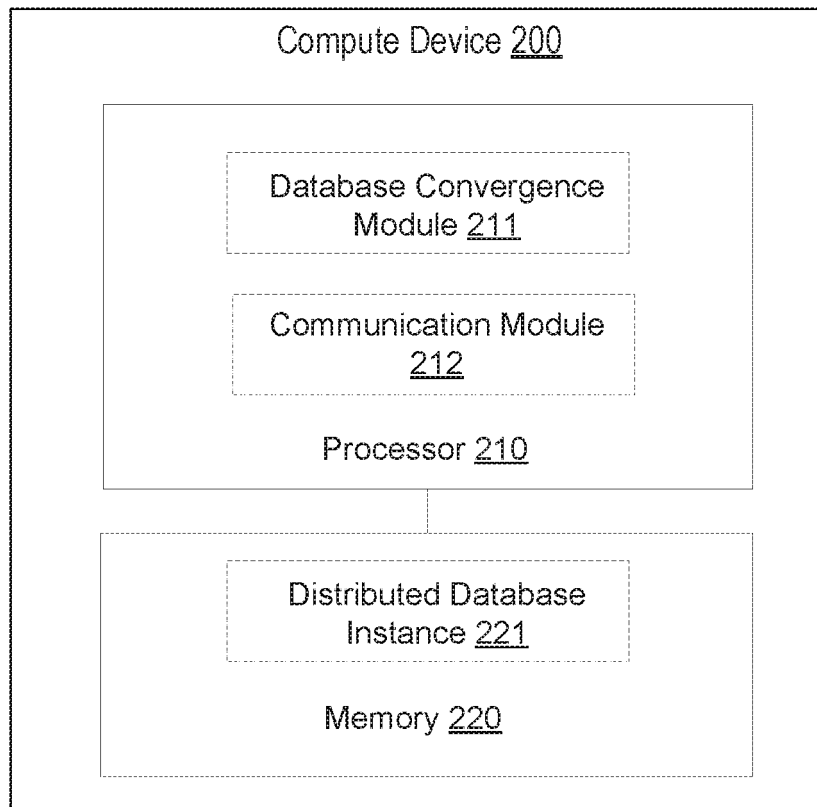


FIG. 2

600

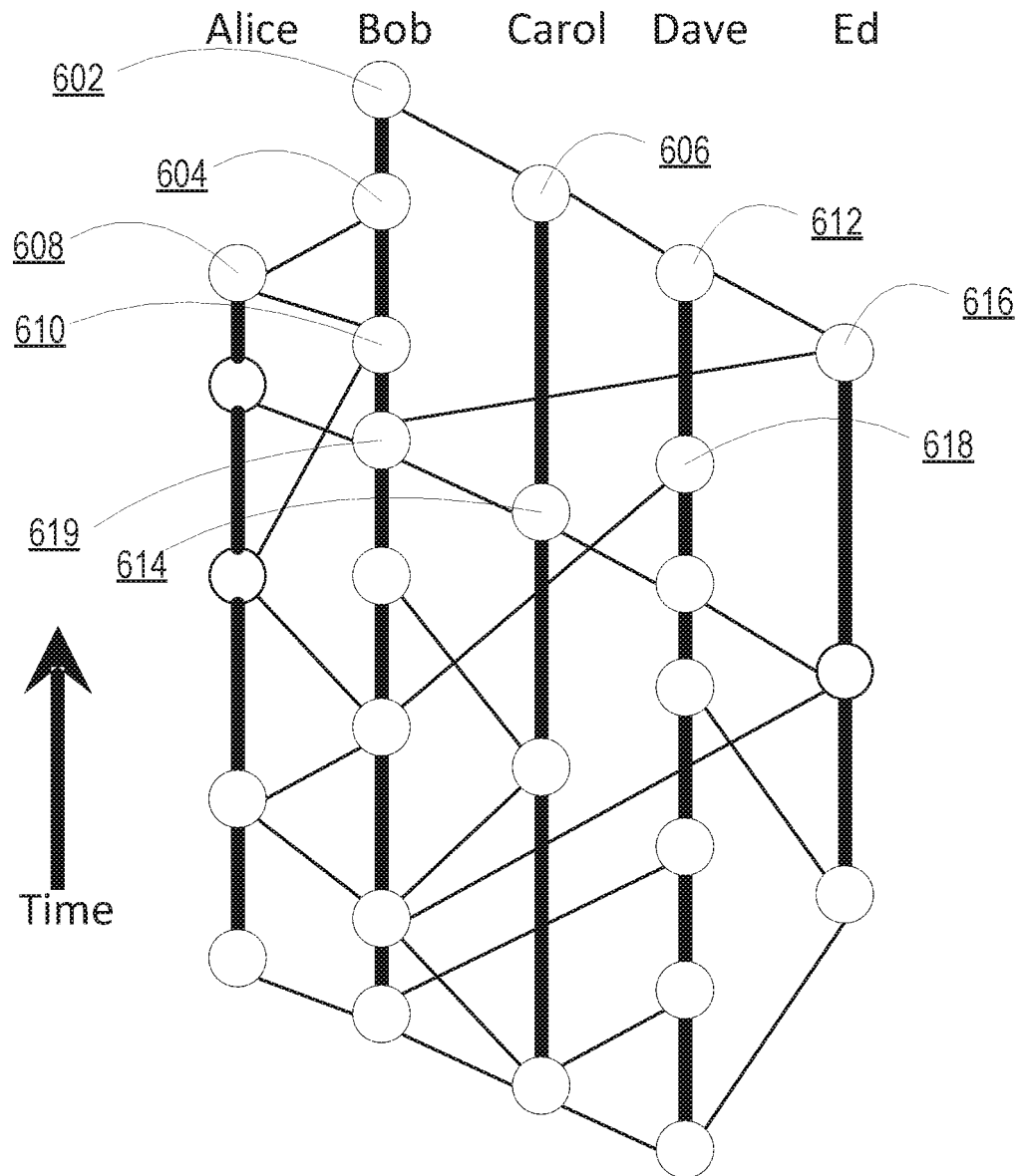


FIG. 3

620

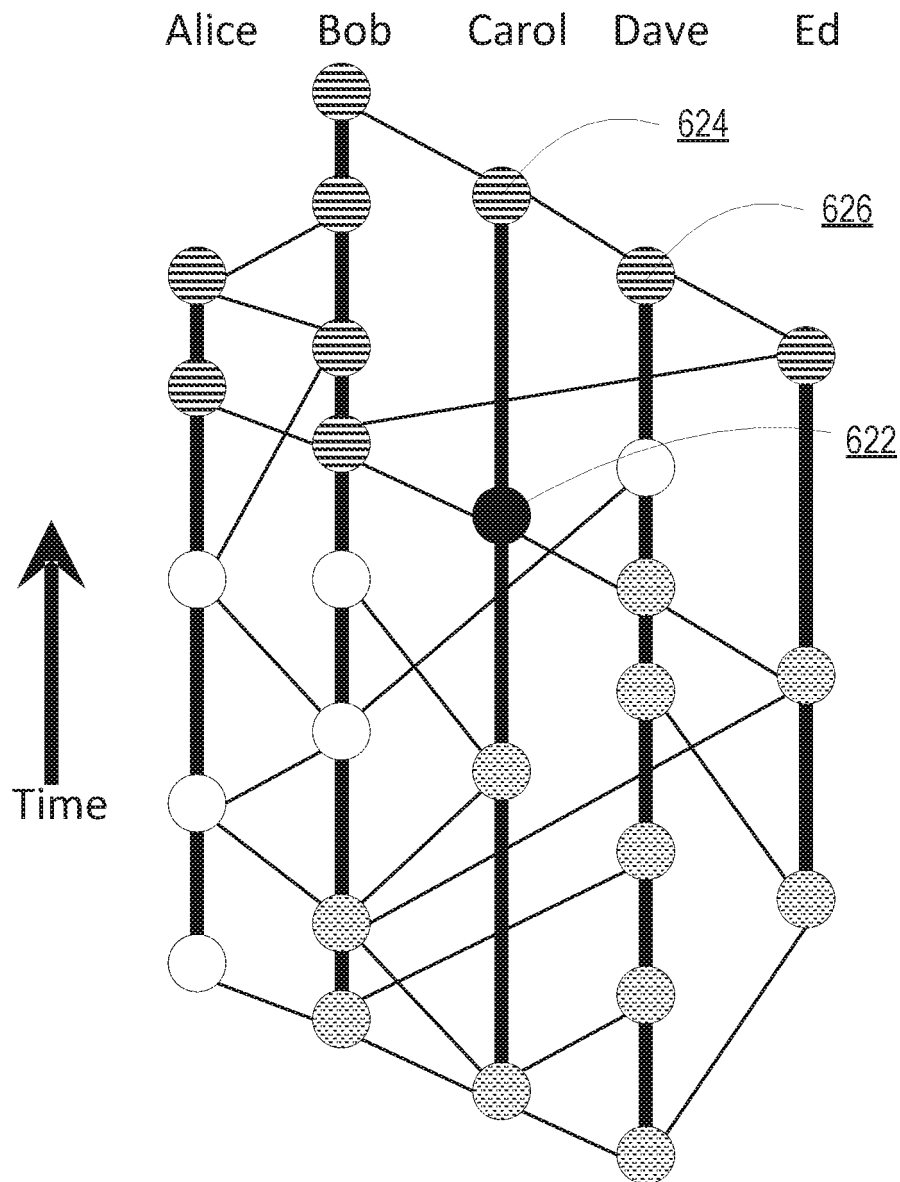


FIG. 4

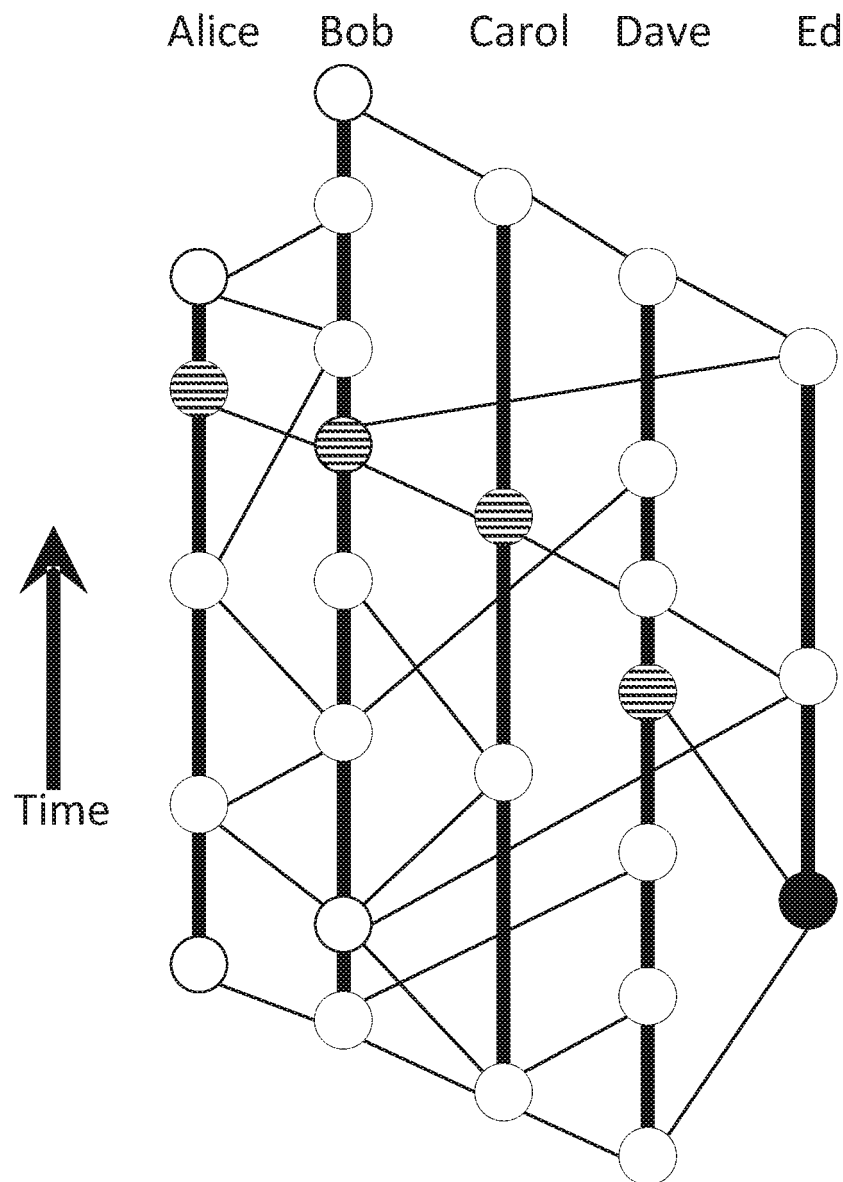


FIG. 5

640

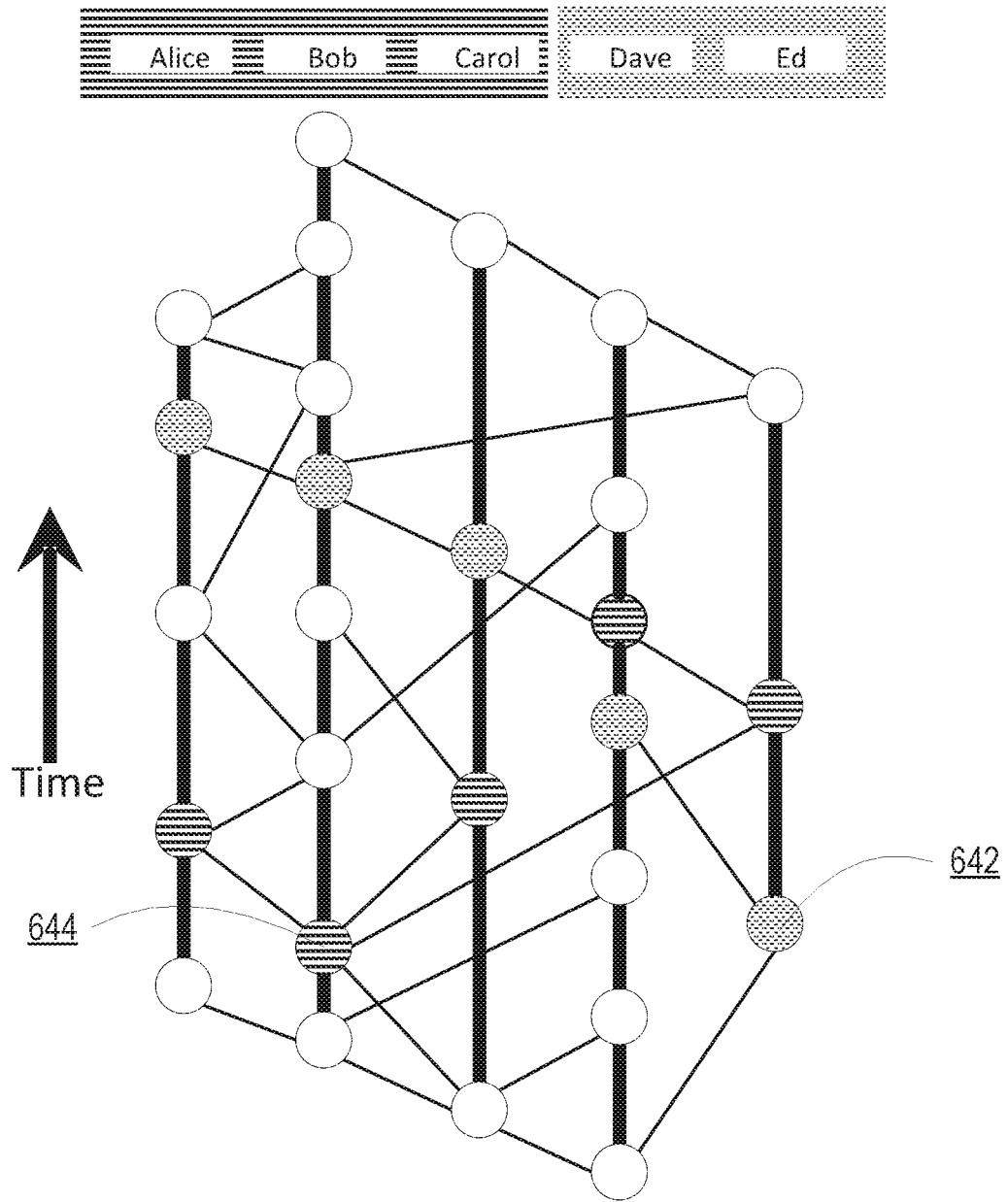


FIG. 6

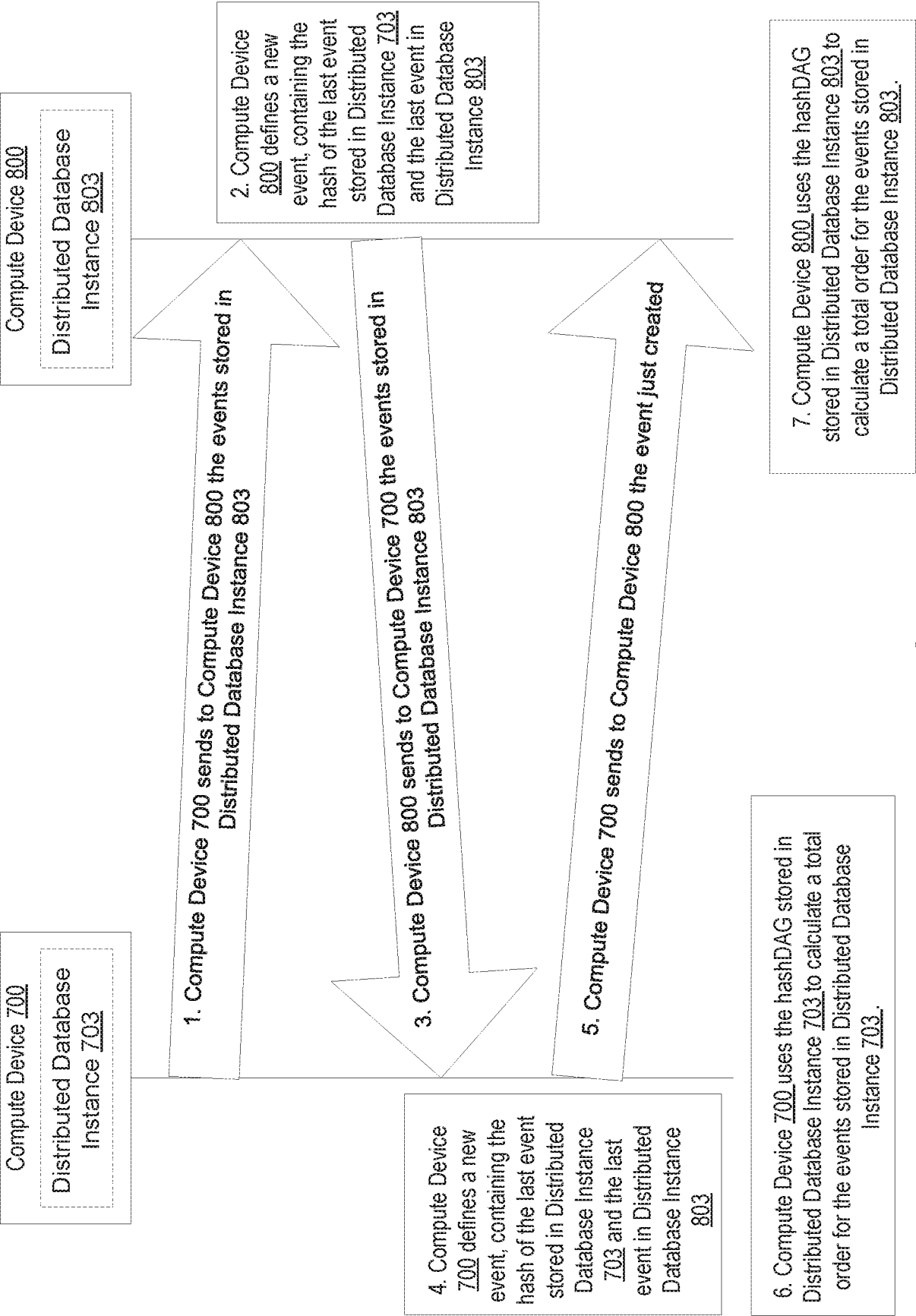


FIG. 7

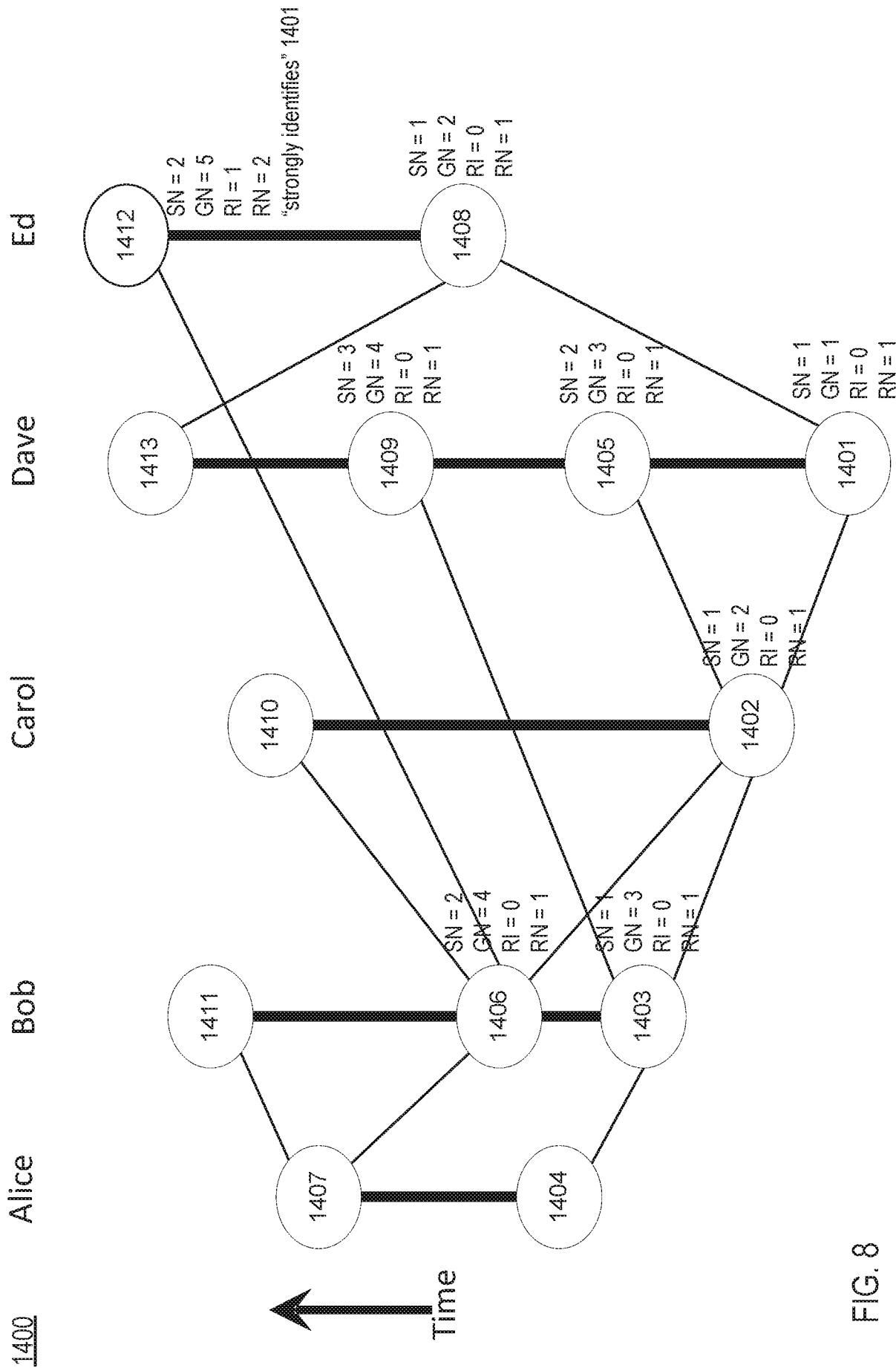
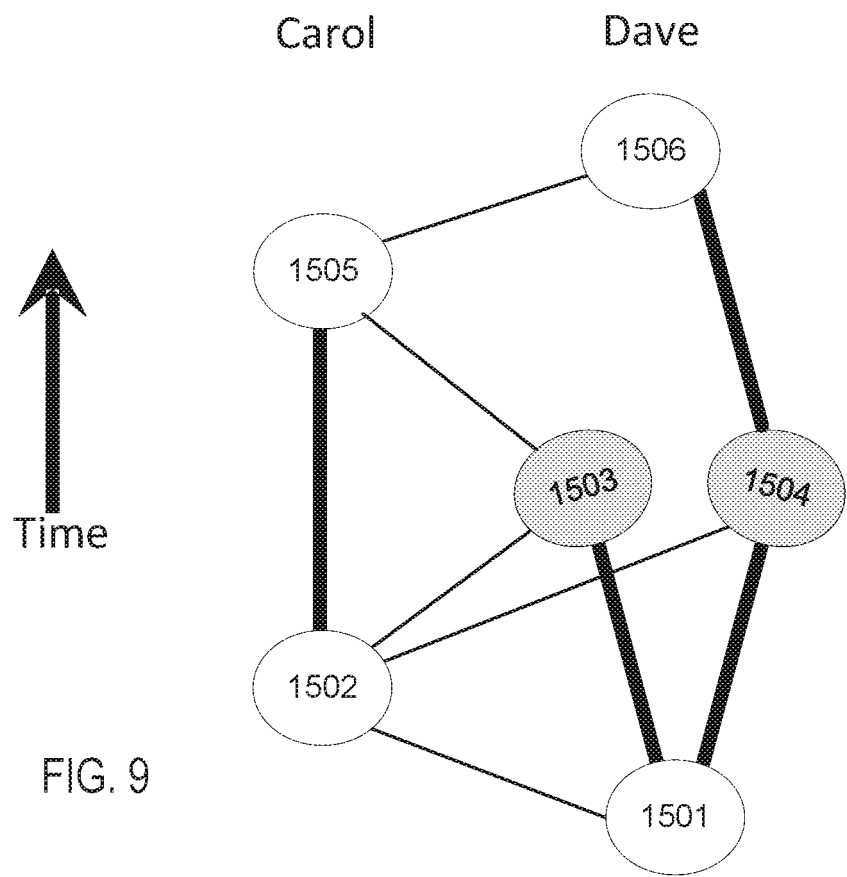


FIG. 8



An event is a tuple $e = \{d, h, t, c, s\}$ where:

d	$= data(e)$	$=$ the “payload” data, which may include transactions.
h	$= hashes(e)$	$=$ a list of hashes of the event’s parents, self-parent first.
t	$= time(e)$	$=$ creator’s claimed date and time of the event’s creation.
c	$= creator(e)$	$=$ creator’s ID number.
s	$= sig(e)$	$=$ creator’s digital signature of $\{d, h, t, c\}$.
n	$=$	the number of members in the population
m	$= 1 + \lfloor 2n/3 \rfloor$	
$first$	$=$	the unique event that has no parents
E	$=$	the set of all events
$\mathbb{T}$	$=$	set of all possible $(time, date)$ pairs
$\mathbb{B}$	$=$	$\{true, false\}$
$\mathbb{N}$	$=$	$\{0, 1, 2, \dots\}$
ancestor	$: E \times E \rightarrow B$	
selfAncestor	$: E \times E \rightarrow B$	
see	$: E \times E \rightarrow B$	
stronglySee	$: E \times E \rightarrow B$	
parentRound	$: E \rightarrow \mathbb{N}$	
witness	$: E \rightarrow \mathbb{B}$	
round	$: E \rightarrow \mathbb{N}$	
roundDiff	$: E \times E \rightarrow \mathbb{I}$	
votes	$: E \times E \times \mathbb{B} \rightarrow \mathbb{N}$	
voteFraction	$: E \times E \rightarrow \mathbb{R}$	
vote	$: E \times E \rightarrow \mathbb{B}$	
decide	$: E \times E \rightarrow \mathbb{B}$	
allFamous	$: \mathbb{I} \rightarrow 2^E$	
famous	$: E \rightarrow \mathbb{B}$	
roundReceived	$: E \rightarrow \mathbb{N}$	
timeReceived	$: E \rightarrow \mathbb{T}$	

FIG. 10A

$$\begin{aligned}
\text{ancestor}(x, y) &= (x = y) \vee (\exists z \in \text{parents}(x) : \text{ancestor}(z, y)) \\
\text{selfAncestor}(x, y) &= \text{ancestor}(x, y) \wedge ((\text{selfParent}(x) = y) \vee \text{selfAncestor}(\text{selfParent}(x), y)) \\
\text{see}(x, y) &= \text{ancestor}(x, y) \wedge \neg(\exists a, b, c \in E : \\
&\quad (\text{ancestor}(y, a) \wedge \text{ancestor}(y, b) \wedge c \in \text{parents}(x) \wedge c \in \text{parents}(b)) \wedge \\
&\quad \text{creator}(a) = \text{creator}(b) = \text{creator}(c)) \\
\text{stronglySee}(x, y) &= \text{see}(x, y) \wedge (\exists S \in 2^E : (|S| = m) \wedge (z \in S \iff (\text{see}(x, z) \wedge \text{see}(z, y)))) \\
\text{parentRound}(x) &= \begin{cases} 0 & \text{if } x = \text{first} \\ \max_{y \in \text{parents}(x)} \text{round}(y) & \text{otherwise} \end{cases} \\
\text{witness}(x) &= \exists S \in 2^E : (|S| = m \wedge \\
&\quad (\forall y \in S : (\text{round}(y) = \text{parentRound}(x) \wedge \text{stronglySee}(x, y)))) \\
\text{round}(x) &= \begin{cases} 1 + \text{parentRound}(x) & \text{if } \text{witness}(x) \\ \text{parentRound}(x) & \text{otherwise} \end{cases} \\
\text{roundDiff}(x, y) &= \text{round}(x) - \text{round}(y) \\
\text{votes}(x, y, v) &= |\{z \in E \mid \text{see}(x, y) \wedge \text{roundDiff}(x, z) = 1 \wedge \\
&\quad \text{stronglySee}(x, z) \wedge \text{vote}(z, y) = v\}| \\
\text{voteFraction}(x, y) &= \text{votes}(x, \text{true}) / (\text{votes}(x, \text{true}) + \text{votes}(x, \text{false})) \\
\text{vote}(x, y) &= \begin{cases} \text{see}(x, y) & \text{if } \text{roundDiff}(x, y) = 1 \\ (\text{voteFraction}(x, y) \geq 1/2) & \text{if } (\text{roundDiff}(x, y) \bmod 5 \neq 1) \vee \\ & |\text{voteFraction}(x, y) - 1/2| > 1/6 \\ (1 = \text{LSB}(\text{signature}(x))) & \text{otherwise} \end{cases} \\
\text{decide}(x, y) &= \text{vote}(x, y) \wedge (\text{roundDiff}(x, y) \bmod 5 \neq 1) \wedge (\text{voteFraction}(x, y) > 2/3) \\
\text{allFamous}(r) &= \{x \in E \mid \text{famous}(x) \wedge \text{round}(x) = r\} \\
\text{famous}(x) &= \text{witness}(x) \wedge \exists y \in E : \text{decide}(y, x) \\
\text{roundReceived}(x) &= \min_{r \in \mathbb{N}} (|\{y \in E \mid \text{round}(y) = r \wedge \text{famous}(y) \wedge \text{see}(y, x)\}| / \\
&\quad |\{y \in E \mid \text{round}(y) = r \wedge \text{famous}(y)\}| \geq 1/2) \\
\text{timeReceived}(x) &= \text{median}(\{\text{time}(y) \mid y \in E \wedge \text{see}(y, x) \wedge \\
&\quad (\exists z \in E : \text{round}(z) = \text{roundReceived}(x) \wedge \text{selfAncestor}(z, y)) \wedge \\
&\quad \neg(\exists w \in E : \text{selfAncestor}(y, w) \wedge \text{see}(w, x))\})
\end{aligned}$$

FIG. 10B

An event is a tuple $e = \{d, h, t, c, s\}$ where:

d	$= data(e)$	$=$ the “payload” data, which may include transactions.
h	$= hashes(e)$	$=$ a list of hashes of the event’s parents, self-parent first.
t	$= time(e)$	$=$ creator’s claimed date and time of the event’s creation.
i	$= creator(e)$	$=$ creator’s ID number.
s	$= sig(e)$	$=$ creator’s digital signature of $\{d, h, t, c\}$.
n	$=$	the number of members in the population
c	$=$	frequency of coin rounds (e.g., $c = 6$)
E	$=$	(the set of all events) $\cup \{\emptyset\}$
T	$=$	set of all possible $(time, date)$ pairs
$\mathbb{B}$	$=$	$\{true, false\}$
$\mathbb{N}$	$=$	$\{0, 1, 2, \dots\}$
parents	:	$E \rightarrow 2^E$
selfParent	:	$E \rightarrow E$
ancestor	:	$E \times E \rightarrow \mathbb{B}$
selfAncestor	:	$E \times E \rightarrow \mathbb{B}$
see	:	$E \times E \rightarrow \mathbb{B}$
stronglySee	:	$E \times E \rightarrow \mathbb{B}$
parentRound	:	$E \rightarrow \mathbb{N}$
roundInc	:	$E \rightarrow \mathbb{B}$
round	:	$E \rightarrow \mathbb{N}$
witness	:	$E \rightarrow \mathbb{B}$
roundDiff	:	$E \times E \rightarrow \mathbb{I}$
votes	:	$E \times E \times \mathbb{B} \rightarrow \mathbb{N}$
fractTrue	:	$E \times E \rightarrow \mathbb{R}$
decide	:	$E \times E \rightarrow \mathbb{B}$
vote	:	$E \times E \rightarrow \mathbb{B}$
famous	:	$E \rightarrow \mathbb{B}$
roundReceived	:	$E \rightarrow \mathbb{N}$
timeReceived	:	$E \rightarrow T$

FIG. 11A

$\text{parents}(x)$	$\equiv$	set of parents of event x
$\text{selfParent}(x)$	$\equiv$	the self-parent of event x , or $\emptyset$ if none
$\text{ancestor}(x, y)$	$\equiv$	$(x \neq \emptyset) \wedge ((x = y) \vee (\exists z \in \text{parents}(x) : \text{ancestor}(z, y)))$
$\text{selfAncestor}(x, y)$	$\equiv$	$(x \neq \emptyset) \wedge ((x = y) \vee \text{selfAncestor}(\text{selfParent}(x), y))$
$\text{see}(x, y)$	$\equiv$	$\text{ancestor}(x, y) \wedge \neg(\exists a, b \in E : \text{creator}(y) = \text{creator}(a) = \text{creator}(b) \wedge \text{ancestor}(x, a) \wedge \text{ancestor}(x, b) \wedge \neg \text{selfAncestor}(a, b) \wedge \neg \text{selfAncestor}(b, a))$
$\text{stronglySee}(x, y)$	$\equiv$	$\text{see}(x, y) \wedge (\exists S \in 2^E : (S > 2n/3 \wedge (z \in S \iff (\text{see}(x, z) \wedge \text{see}(z, y))))$
$\text{parentRound}(x)$	$\equiv$	$\max(\{0\} \cup \{\text{round}(y) y \in \text{parents}(x)\})$
$\text{roundInc}(x)$	$\equiv$	$\exists S \in 2^E : (S > 2n/3 \wedge (\forall y \in S : (\text{round}(y) = \text{parentRound}(x) \wedge \text{stronglySee}(x, y))))$
$\text{round}(x)$	$\equiv$	$\text{parentRound}(x) + \begin{cases} 1 & \text{if } \text{roundInc}(x) \\ 0 & \text{otherwise} \end{cases}$
$\text{witness}(x)$	$\equiv$	$(\text{selfParent}(x) = \emptyset) \vee (\text{round}(x) > \text{round}(\text{selfParent}(x)))$
$\text{roundDiff}(x, y)$	$\equiv$	$\text{round}(x) - \text{round}(y)$
$\text{votes}(x, y, v)$	$\equiv$	$ \{z \in E \mid \text{roundDiff}(x, z) = 1 \wedge \text{stronglySee}(x, z) \wedge \text{vote}(z, y) = v\} $
$\text{fractTrue}(x, y)$	$\equiv$	$\frac{\text{votes}(x, y, \text{true})}{(\text{votes}(x, y, \text{true}) + \text{votes}(x, y, \text{false}))}$
$\text{decide}(x, y)$	$\equiv$	$(x \neq \emptyset) \wedge (\text{roundDiff}(x, y) > 1) \wedge (\text{decide}(\text{selfParent}(x), y) \vee (\text{witness}(x) \wedge (\text{roundDiff}(x, y) \bmod c \neq 1) \wedge \neg(\frac{1}{3} \leq \text{fractTrue}(x, y) \leq \frac{2n}{3})))$
$\text{vote}(x, y)$	$\equiv$	$\begin{cases} \text{vote}(\text{selfParent}(x), y) & \text{if } (\neg \text{witness}(x)) \vee \text{decide}(\text{selfParent}(x), y) \\ 1 = \text{middleBit}(\text{signature}(x)) & \text{if } \text{witness}(x) \\ & \wedge \neg \text{decide}(\text{selfParent}(x), y) \\ & \wedge (\text{roundDiff}(x, y) \neq 1) \\ & \wedge (\text{roundDiff}(x, y) \bmod c = 1) \\ \text{fractTrue}(x, y) \geq \frac{1}{2} & \text{otherwise} \end{cases}$
$\text{famous}(x)$	$\equiv$	$\text{witness}(x) \wedge \exists y \in E : \text{decide}(y, x) \wedge \text{vote}(y, x)$
$\text{roundReceived}(x)$	$\equiv$	$\min_{r \in \mathbb{N}} \frac{ \{y \in E \mid (\text{round}(y) = r) \wedge \text{famous}(y) \wedge \text{see}(y, x)\} }{ \{y \in E \mid (\text{round}(y) = r) \wedge \text{famous}(y)\} } \geq 1/2$
$\text{timeReceived}(x)$	$\equiv$	$\text{median}(\{\text{time}(y) \mid y \in E \wedge \text{see}(y, x) \wedge (\exists z \in E : \text{round}(z) = \text{roundReceived}(x) \wedge \text{selfAncestor}(z, y)) \wedge \neg(\exists w \in E : \text{selfAncestor}(y, w) \wedge \text{see}(w, x))\})$

FIG. 11B

An event is a tuple $e = \{d, h, t, i, s\}$ where:

d	$= data(e)$	$=$ the “payload” data, which may include transactions.
h	$= hashes(e)$	$=$ a list of hashes of the event’s parents, self-parent first.
t	$= time(e)$	$=$ creator’s claimed date and time of the event’s creation.
i	$= creator(e)$	$=$ creator’s ID number.
s	$= sig(e)$	$=$ creator’s digital signature of $\{d, h, t, i\}$.
$parents(x)$	$=$	set of events that are parents of event x
$selfParent(x)$	$=$	the self-parent of event x , or $\emptyset$ if none
n	$=$	the number of members in the population
c	$=$	frequency of coin rounds (such as $c = 10$)
E	$=$	the set of all events in the hashgraph
E_0	$=$	$E \cup \{\emptyset\}$
$\mathbb{T}$	$=$	set of all possible $(time, date)$ pairs
$\mathbb{B}$	$=$	$\{true, false\}$
$\mathbb{N}$	$=$	$\{1, 2, 3, \dots\}$
$parents$	$:$	$E \rightarrow 2^E$
$selfParent$	$:$	$E \rightarrow E_0$
$ancestor$	$:$	$E \times E \rightarrow \mathbb{B}$
$selfAncestor$	$:$	$E \times E \rightarrow \mathbb{B}$
$manyCreators$	$:$	$2^E \rightarrow \mathbb{B}$
see	$:$	$E \times E \rightarrow \mathbb{B}$
$stronglySee$	$:$	$E \times E \rightarrow \mathbb{B}$
$parentRound$	$:$	$E \rightarrow \mathbb{N}$
$roundInc$	$:$	$E \rightarrow \mathbb{B}$
$round$	$:$	$E \rightarrow \mathbb{N}$
$witness$	$:$	$E \rightarrow \mathbb{B}$
$diff$	$:$	$E \times E \rightarrow \mathbb{I}$
$votes$	$:$	$E \times E \times \mathbb{B} \rightarrow \mathbb{N}$
$fractTrue$	$:$	$E \times E \rightarrow \mathbb{R}$
$decide$	$:$	$E \times E \rightarrow \mathbb{B}$
$copyVote$	$:$	$E \times E \rightarrow \mathbb{B}$
$vote$	$:$	$E \times E \rightarrow \mathbb{B}$
$famous$	$:$	$E \rightarrow \mathbb{B}$
$uniqueFamous$	$:$	$E \rightarrow \mathbb{B}$
$roundsDecided$	$:$	$\mathbb{N} \rightarrow \mathbb{B}$
$roundReceived$	$:$	$E \rightarrow \mathbb{N}$
$timeReceived$	$:$	$E \rightarrow \mathbb{T}$

FIG. 12A

$$\begin{aligned}
\text{ancestor}(x, y) &= x = y \vee \exists z \in \text{parents}(x), \text{ancestor}(z, y) \\
\text{selfAncestor}(x, y) &= x = y \vee (\text{selfParent}(x) \neq \emptyset \wedge \text{selfAncestor}(\text{selfParent}(x), y)) \\
\text{manyCreators}(S) &= |S| > 2n/3 \wedge \forall x, y \in S, (x \neq y \implies \text{creator}(x) \neq \text{creator}(y)) \\
\text{see}(x, y) &= \text{ancestor}(x, y) \wedge \neg(\exists a, b \in E, \text{creator}(y) = \text{creator}(a) = \text{creator}(b) \wedge \\
&\quad \text{ancestor}(x, a) \wedge \text{ancestor}(x, b) \wedge \neg \text{selfAncestor}(a, b) \wedge \neg \text{selfAncestor}(b, a)) \\
\text{stronglySee}(x, y) &= \text{see}(x, y) \wedge (\exists S \subseteq E, \text{manyCreators}(S) \\
&\quad \wedge (z \in S \implies (\text{see}(x, z) \wedge \text{see}(z, y)))) \\
\text{parentRound}(x) &= \max(\{1\} \cup \{\text{round}(y) \mid y \in \text{parents}(x)\}) \\
\text{roundInc}(x) &= \exists S \subseteq E, \text{manyCreators}(S) \\
&\quad \wedge (\forall y \in S, \text{round}(y) = \text{parentRound}(x) \wedge \text{stronglySee}(x, y)) \\
\text{round}(x) &= \text{parentRound}(x) + \begin{cases} 1 & \text{if } \text{roundInc}(x) \\ 0 & \text{otherwise} \end{cases} \\
\text{witness}(x) &= (\text{selfParent}(x) = \emptyset) \vee (\text{round}(x) > \text{round}(\text{selfParent}(x))) \\
\text{diff}(x, y) &= \text{round}(x) - \text{round}(y) \\
\text{votes}(x, y, v) &= |\{z \in E \mid \text{diff}(x, z) = 1 \wedge \text{witness}(z) \wedge \text{stronglySee}(x, z) \wedge \text{vote}(z, y) = v\}| \\
\text{fractTrue}(x, y) &= \frac{\text{votes}(x, y, \text{true})}{(\text{votes}(x, y, \text{true}) + \text{votes}(x, y, \text{false}))} \\
\text{decide}(x, y) &= (\text{selfParent}(x) \neq \emptyset \wedge \text{decide}(\text{selfParent}(x), y)) \vee (\wedge \text{witness}(x) \wedge \text{witness}(y) \\
&\quad \wedge \text{diff}(x, y) > 1 \wedge (\text{diff}(x, y) \bmod c > 0) \wedge (\exists v \in B, \text{votes}(x, y, v) > \frac{2n}{3})) \\
\text{copyVote}(x, y) &= (\neg \text{witness}(x)) \vee (\text{selfParent}(x) \neq \emptyset \wedge \text{decide}(\text{selfParent}(x), y)) \\
\text{vote}(x, y) &= \begin{cases} \text{vote}(\text{selfParent}(x), y) & \text{if } \text{copyVote}(x) \\ 1 = \text{middleBit}(\text{signature}(x)) & \text{if } \neg \text{copyVote}(x) \\ \quad \wedge (\text{diff}(x, y) \bmod c = 0) \\ \quad \wedge (\frac{1}{3} \leq \text{fractTrue}(x, y) \leq \frac{2}{3}) \\ \text{fractTrue}(x, y) \geq \frac{1}{2} & \text{otherwise} \end{cases} \\
\text{famous}(x) &= \exists y \in E, \text{decide}(y, x) \wedge \text{vote}(y, x) \\
\text{uniqueFamous}(x) &= \text{famous}(x) \wedge \neg \exists y \in E, y \neq x \wedge \text{famous}(y) \\
&\quad \wedge \text{round}(x) = \text{round}(y) \wedge \text{creator}(x) = \text{creator}(y) \\
\text{roundsDecided}(r) &= \forall x \in E, ((\text{round}(x) \leq r \wedge \text{witness}(x)) \implies \exists y \in E, \text{decide}(y, x)) \\
\text{roundReceived}(x) &= \min(\{r \in \mathbb{N} \mid \text{roundsDecided}(r) \wedge (\forall y \in E, \\
&\quad (\text{round}(y) = r \wedge \text{uniqueFamous}(y)) \implies \text{ancestor}(y, x)\}) \\
\text{timeReceived}(x) &= \text{median}(\{\text{time}(y) \mid y \in E \wedge \text{ancestor}(y, x) \wedge \\
&\quad (\exists z \in E, \text{round}(z) = \text{roundReceived}(x) \wedge \text{uniqueFamous}(z) \\
&\quad \wedge \text{selfAncestor}(z, y)) \wedge \neg(\exists w \in E, \text{selfAncestor}(y, w) \wedge \text{ancestor}(w, x))\})
\end{aligned}$$

FIG. 12B

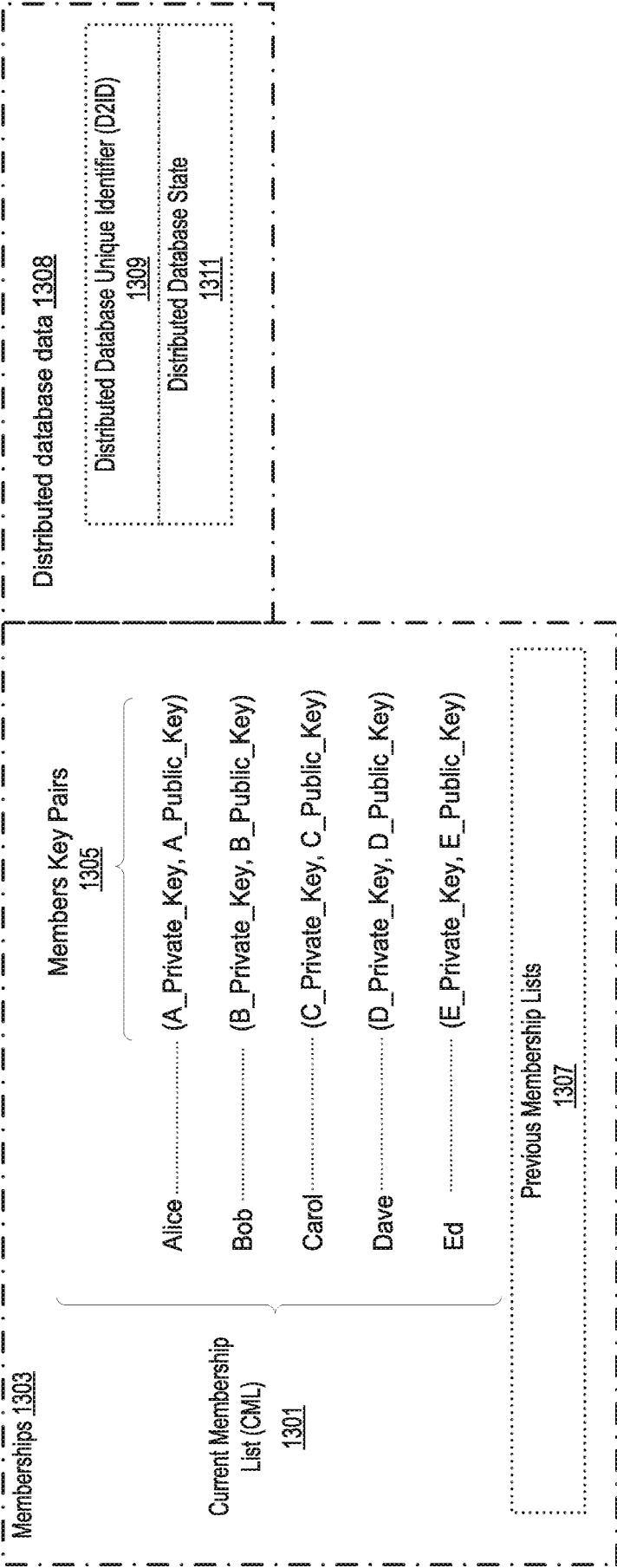


FIG. 13

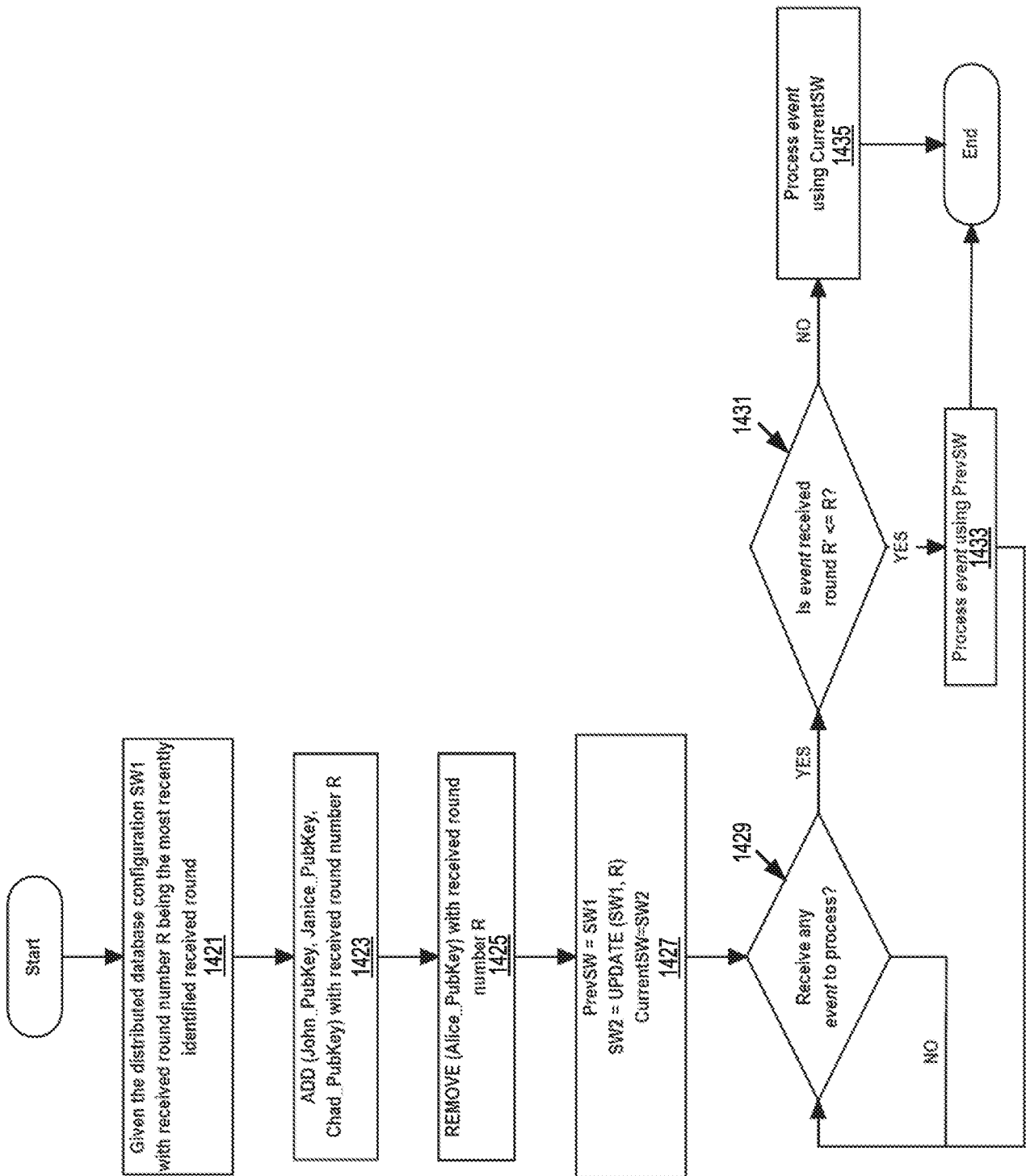


FIG. 14

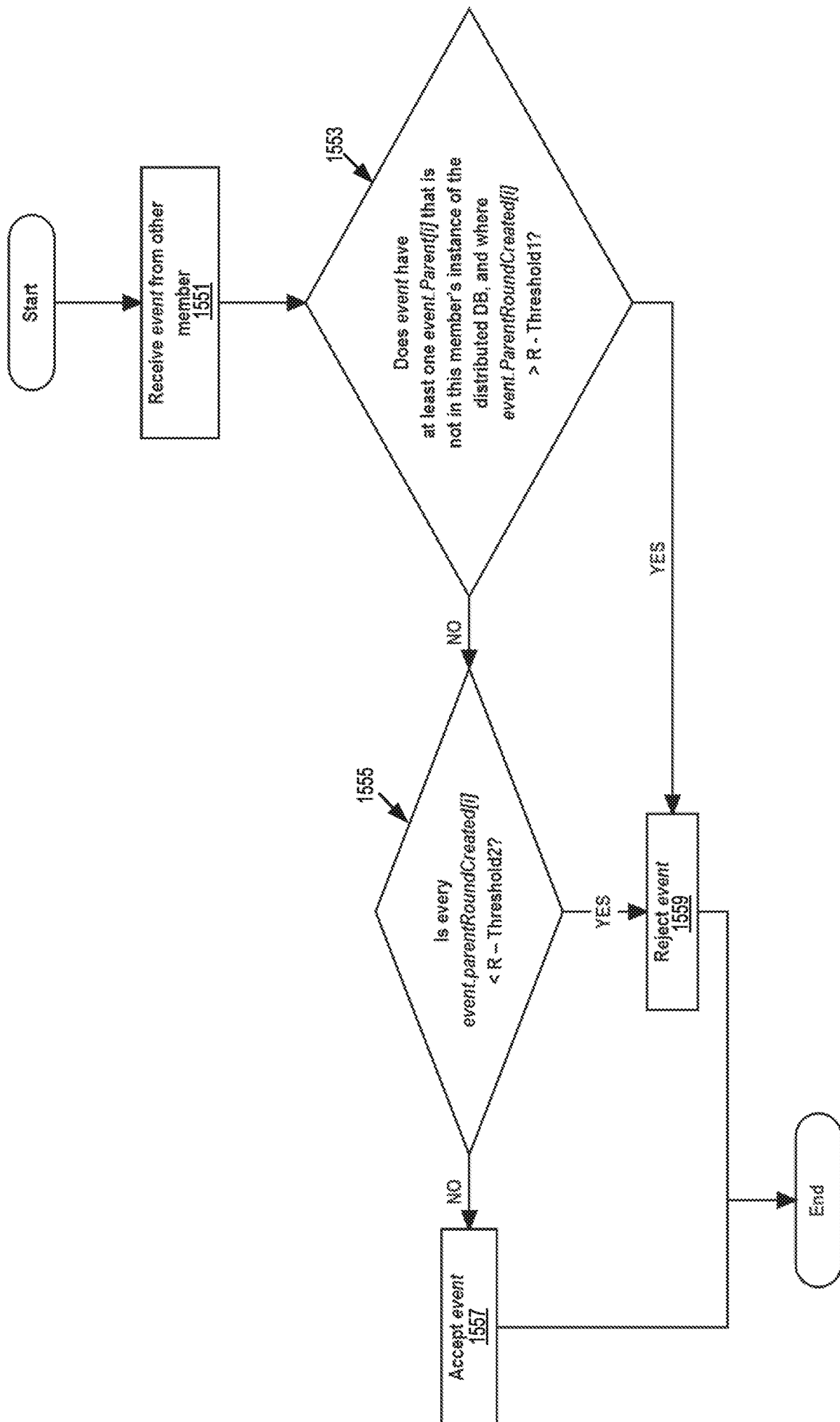


FIG. 15

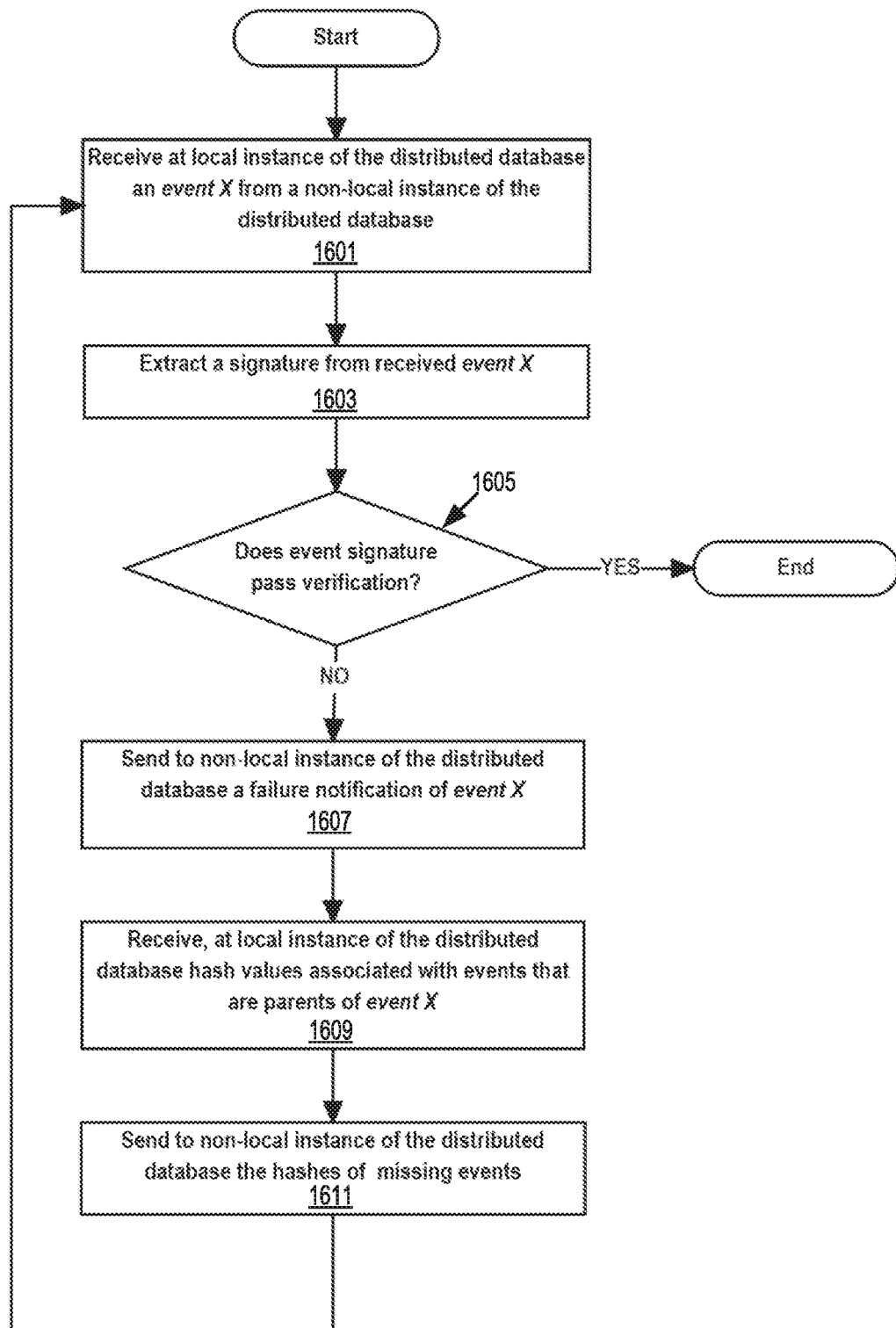


FIG. 16